

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-202336

(43)Date of publication of application : 27.07.2001

(51)Int.Cl.

G06F 15/00

H04L 9/32

(21)Application number : 2000-011844

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

(22)Date of filing : 20.01.2000

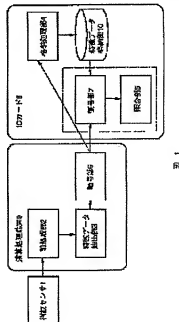
(72)Inventor : MURAYAMA TAKAHIKO
KAKU NICHIKO
HOSODA YASUHIRO

(54) METHOD FOR AUTHENTICATING IDENTITY AND DEVICE FOR EXECUTING THE SAME

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a method for authenticating identity and a device for executing the same, with which security is extremely improved by preventing the embezzlement of a card and excluding the embezzlement of personal feature data in the use of the card as well.

SOLUTION: Concerning the method for authenticating identity and the device for executing the same, the data of specified personal physical features are previously registered on an IC card 8, the data of physical features provided from the carrying person of this IC card 8 are transmitted to the IC card 8, these transmitted data of physical features are collated with the previously registered data of physical features inside the IC card 8, and it is authenticated whether a person carrying the relevant IC card 8 is the person having the physical features registered on the relevant IC card or not.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-202336

(P2001-202336A)

(43) 公開日 平成13年7月27日 (2001.7.27)

(51) Int.Cl. ⁷	識別記号	F I	テート ⁷ (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 F 5 B 0 8 5
			3 3 0 G 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A
			6 7 3 D
			6 7 3 E
審査請求 未請求 請求項の数 6 O L (全 6 頁)			

(21) 出願番号 特願2000-11844(P2000-11844)

(22) 出願日 平成12年1月20日 (2000.1.20)

(71) 出願人 000004228

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 村山 隆彦

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(73) 発明者 堀 日洪

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100066153

弁理士 草野 卓 (外1名)

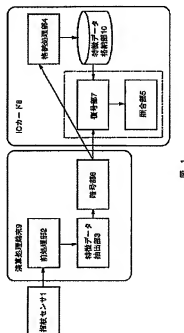
最終頁に続く

(54) 【発明の名称】 本人認証方法およびこの方法を実施する装置

(57) 【要約】

【課題】

【解決手段】 ICカード8に特定の個人の身体的特徴のデータを事前に登録しておき、このICカード8の携帯者から得た身体的特徴のデータをICカード8に送信し、この送信された身体的特徴のデータと事前に登録されている身体的特徴のデータとをICカード8内において照合し、当該ICカード8の携帯者が当該ICカードに身体的特徴を登録されている本人であるか否かを認証する本人認証方法およびこの方法を実施する装置。



【請求項の範囲】

【請求項1】 ICカードに特定の個人の身体的特徴のデータを事前に登録しておき、このICカードの携帯者から得た身体的特徴のデータをICカードに送信し、この送信された身体的特徴のデータと事前に登録されている身体的特徴のデータとをICカード内において照合し、当該ICカードの携帯者が当該ICカードに身体的特徴を登録されている本人であるか否かを認証することを特徴とする本人認証方法。

【請求項2】 請求項1に記載される本人認証方法において、身体的特徴のデータは、指紋、声紋、虹彩、筆跡その他のバイOMETRICSデータから選択した何れか1個、或いは複数個の組み合わせであることを特徴とする本人認証方法。

【請求項3】 身体的特徴を検出するセンサを具備し、センサにより読み取られた画像データを入力して特徴データを抽出する特徴データ抽出部を有する演算処理端末を具備し、演算処理端末から特徴データを入力して格納処理する格納処理部と、特徴データを記憶する特徴データ格納部と、演算処理端末から特徴データを入力すると共に特徴データ格納部から読み出される特徴データを入力して両データを比較照合して照合結果を出力する照合部より成るICカードを具備することを特徴とする本人認証装置。

【請求項4】 請求項3に記載される本人認証装置において、演算処理端末は特徴データ抽出部に前置され、入力される画像データのデジタル化、画像の色数の削減、ノイズの除去、画像の位置補正その他の前処理を行う前処理部を具備することを特徴とする本人認証装置。

【請求項5】 請求項3および請求項4の内の何れかに記載される本人認証装置において、演算処理端末は特徴データ抽出部より抽出された特徴データを暗号化する暗号部を具備し、ICカードは演算処理端末の暗号部から出力される暗号化された特徴データを入力すると共に特徴データ格納部に格納されている暗号化されている特徴データを読み出し入力して両特徴データを復号化する復号部を具備することを特徴とする本人認証装置。

【請求項6】 請求項3ないし請求項5の内の何れかに記載される本人認証装置において、ICカードにおける特徴データの登録読み出し処理、復号化処理、比較照合処理はICカードの内蔵するCPUの照合プログラムにより実施する構成とすることを特徴とする本人認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、本人認証方法お

よびこの方法を実施する装置に関し、特に、ICカードの盗用を防止すると共にICカード使用時における個人の特征データの盗聴も排除する極めてセキュリティの高い本人認証方法およびこの方法を実施する装置に関する。

【0002】

【従来の技術】キャッシュディスプレイ、ネットワーク上のサーバにアクセスし、或いは駐車場、コンピュータ室、一般のオフィスの如き領域に入場し、或はここから退出する場合、携帯者が本人であるものとするIDカードの如き本人認証カードが使用されている。また、IDカードを携帯することの他に、更に4桁程度の暗証番号を併用して本人であるか否かを認める方法が採用されている。ところが、IDカードを紛失し、IDカードの盗難に遭遇すると、IDカードの盗用、暗証番号の盗用により、他人が本人になります事故が発生する。近時、この種の事故が増加しており、これに対する有効な対策が望まれている。

【0003】ここで、本人確認の手法として、IDカード或いは暗証番号と比較して遙かに有効である指紋、声紋、虹彩、筆跡その他のバイOMETRICSデータである身体的特徴のデータを使用する方法が開発、使用されている。これを図4を参照して説明する。図4において、指紋センサ1は、指紋を指紋データとして読み取り、これをA/D変換した画像データを生ずるものである。

【0004】CPUにより構成される演算処理端末9は、指紋センサ1により読み取られ、A/D変換された画像データが入力される。演算処理端末9の前処理部2は、入力された画像データの色数を削減し、画像の濃淡を2値化すると共に、ノイズを除去/平滑化し、画像の輪郭を細線化して画像データを整形する。前処理部2は更に、指紋データ登録時の画像と指紋データ照合時の画像との間の位置補正を行う。特徴データ抽出部3は、前処理された画像データを入力して指紋模様の特徴点、端点その他の特徴点を抽出し、抽出された特徴点間の位置関係の演算処理を行う。6は暗号部であり、特徴データ抽出部3により抽出された特徴データを入力してこれを暗号に変換するところである。以上の前処理部2、特徴データ抽出部3、暗号部6が演算処理端末9の内のカード発行部を形成している。照合部5は、特徴データ抽出部3により抽出された特徴データを入力すると共に復号部7において復号化された特徴データを入力し、両特徴データを比較照合するところである。先のカード発行部に照合部5および復号部7を含めて認証部を構成している。

【0005】ICカード8は、演算処理端末9の暗号部6において暗号化された特徴データを入力してこれを格納処理する格納処理部4と、特徴データを記憶する特徴データ格納部10とより成る。図示されていないが、ICカード8は格納処理部4に対する登録データの格納

読み出し、その他、ICカード8側における各種の演算処理を実行するCPUに内蔵している。ここで、図2を参照して指紋データ1Cカードに登録する場合の処理を説明する。なお、ICカードの登録処理は演算処理端末9に付設されるリーダ/ライタを介して実施される。指紋の画像入力11は、指紋センサ1により、指紋の画像データとして読み取られ、この画像データは、次いでA/D変換される。A/D変換された画像データは演算処理端末9に入力され、前処理部2において前処理12を施される。前処理12を施された画像データは、特徴データ抽出部3に入力され、特徴データ抽出13が実施される。特徴データ抽出部3により抽出された特徴データは暗号部6において暗号化され、暗号化された特徴データは演算処理端末9側からICカード8側に特徴データ送信14される。ICカード8は、暗号化された特徴データを受信し、この受信特徴データを格納処理部4を介して特徴データ格納部10に特徴データ格納15する。

【0006】次に、カード携帯者の指紋データと当該カードに格納されている特徴データの照合をする場合の処理を説明する。特徴データの照合処理も演算処理端末9に付設されるリーダ/ライタを介して実施される。画像入力11から特徴データ送信14までは指紋データ登録の場合と共通している。照合部5は、特徴データ抽出部3により抽出された特徴データを入力すると共に、携帯者のICカード8の特徴データ格納部10に登録されている特徴データを復号部7において復号化して入力し、両特徴データと比較照合する。照合部5は、両特徴データの比較結果がある閾値より大きければ照合成功、閾値より小さければ照合失敗とする。

【0007】以上の従来例においては、特徴データ抽出部3により抽出された特徴データは演算処理端末9の暗号部6において暗号化され、ICカード8の特徴データ格納部10には暗号化された特徴データが格納されているが、この暗号部6を具備せずに特徴データ抽出部3により抽出された特徴データをそのままICカード8に送信してこれを特徴データ格納部10に格納することもできる。この場合、復号部7も省略される。

【0008】

【発明が解決しようとする課題】事前に登録する本人の特徴データは、セキュリティの観点から、不適切な登録データ読み出し処理を実行しようとする自身が破壊するに到る構成とされたICカードに格納しておくことが望ましい。ところが、このICカードは、データとして暗証番号を格納しておく場合と比較してデータ量が大きく、照合に関する計算量も大きいところから、照合時には、アクセスしようとするサーバ或は演算処理端末側にICカードから登録データを読み出して照合を実施することが一般的に行われている。照合時に登録データがICカードの外部に読み出されるということは、ICカー

ド内の登録データ自体の管理に高いセキュリティを求めてみて、これを無意味にする恐れがある。

【0009】この発明は、カードの盗用を防止すると共にカード使用時における個人の特徴データの盗難も排除する極めてセキュリティの高い上述の問題を解消した本人認証方法およびこの方法を実施する装置を提供するものである。

【0010】

【課題を解決するための手段】請求項1：ICカード8に特定の個人の身体的特徴のデータを事前に登録しておき、このICカードの携帯者から得た身体的特徴のデータをICカードに送信し、この送信された身体的特徴のデータと事前に登録されている身体的特徴のデータとをICカード内において照合し、当該ICカードの携帯者が当該ICカードに身体的特徴を登録されている本人であるか否かを認証する本人認証方法を構成した。

【0011】そして、請求項2：請求項1に記載される本人認証方法において、身体的特徴のデータは、指紋、声紋、虹彩、筆跡その他のバイオメトリクスデータから選択した何れか1個、或いは複数個の組み合わせである本人認証方法を構成した。ここで、請求項3：身体的特徴を抽出するセンサ1を具備し、センサ1により読み取られた画像データを入力して特徴データを抽出する特徴データ抽出部3を有する演算処理端末9を具備し、演算処理端末9から特徴データを入力して格納処理する格納処理部4と、特徴データを記憶する特徴データ格納部10と、演算処理端末9から特徴データを入力すると共に特徴データ格納部10から読み出される特徴データを入力して両データを比較照合して照合結果を出力する照合部5より成るICカード8を具備する本人認証装置を構成した。

【0012】そして、請求項4：請求項3に記載される本人認証装置において、演算処理端末9は特徴データ抽出部3に前置され、入力される画像データのデジタル化、画像の色度の削減、ノイズの除去、画像の位置補正その他の前処理を行う前処理部を具備する本人認証装置を構成した。また、請求項5：請求項3および請求項4の内の何れかに記載される本人認証装置において、演算処理端末9は特徴データ抽出部3により抽出された特徴データを暗号化する暗号部6を具備し、ICカード8は演算処理端末9の暗号部6から出力される暗号化された特徴データを入力すると共に特徴データ格納部10に格納されている暗号化された特徴データを読み出し入力して両特徴データを復号化する復号部7を具備する本人認証装置を構成した。

【0013】更に、請求項6：請求項3ないし請求項5の内の何れかに記載される本人認証装置において、ICカード8における特徴データの登録読み出し処理、暗号化処理、比較照合処理はICカード8の内蔵するCPUの照合プログラムにより実施する構成とする本人認証装

図を構成した。

【0014】

【発明の実施の形態】この発明は、ICカード内に、そのカードを所有する個人の身体的特徴のデータ、例えば、指紋、声紋、虹彩、掌紋などのデータを登録しておき、カードの所有者と同一であるか否か分からないカードの持筆者から得た同様の身体的特徴のデータをそのICカードに送り、ICカード内で照合して、カードの持筆者が、カードの所有者と同一であるか否かを判断する。ICカードに組み込まれるCPUの演算処理能力は、身体的特徴のデータを処理するには未だ不充分であるところから、アクセスしようとするサーバ或は演算処理端末側において読み取られた画像データに前処理を施し、ICカード内における演算処理量を極力減らすことが有効である。ここで、前処理とは、画像データのデジタル化、画像の色数の削減、ノイズの除去、画像の位置補正その他の、ICカード内の登録データを利用しないで処理可能な処理であり、また、照合精度を極力落とさない処理を意味する。ICカード内に格納されている登録データは、ICカード8に内蔵されるCPUが有するICカード8固有の照合プログラムからのみアクセスすることができる構成とし、一切ICカードから外へ出力されることはない。更に、ICカードへの転送読み出しデータは、これを暗号化することにより、よりセキュリティを高めることができる。

【0015】

【実施例】この発明の実施例を図1を参照して説明する。図1の実施例において、図4の従来例の部材と共通する部材には共通する参照符号を付与している。図1の実施例において、演算処理端末9は、前処理部2、特徴データ抽出部3および暗号部6より成るカード発行部のみにより構成されている。カード持筆者の指紋データと当該カードに格納されている特徴データの照合をする照合部5および復号部7より成る図4において1点鎖線により区別される認証部を具備していない。

【0016】図1の実施例において、照合部5および復号部7より成る認証部1Cカード8の側に具備されている。即ち、ICカード8は、演算処理端末9の暗号部6において暗号化された特徴データを入力して格納処理する格納処理部4と、特徴データを記憶する特徴データ格納部10と、演算処理端末9の暗号部6において暗号化された特徴データを入力すると共に特徴データ格納部10に格納されている暗号化された特徴データを入力して両特徴データを復号化する復号部7と、復号部7において復号化された両特徴データを比較照合して照合結果を出力する照合部5より成る。

【0017】特徴データ抽出部3により抽出された特徴データは演算処理端末9の暗号部6において暗号化され、ICカード8の特徴データ格納部10には暗号化された特徴データが格納されているが、この暗号部6を具

備せずに特徴データ抽出部3により抽出された特徴データをそのままICカード8の格納処理部4に送信してこれを特徴データ格納部10に格納する。この場合、ICカード8において復号部7は省略され、照合に際して特徴データをそのまま照合部5に送信する。暗号部6および復号部7を具備することによりセキュリティレベルはより向上する。

【0018】ここで、図1の実施例における指紋データのICカードに対する登録は、図4の従来例の場合と同様に実施される。図3を参照してカード持筆者の指紋データと当該カードに格納されている特徴データの照合をする場合の処理を説明する。ICカードの登録処理は、従来例と同様に、演算処理端末9に付設されるリーダー/ライタを介して実施される。指紋の画像入力11は、指紋センサ1により、指紋の画像データとして読み取られ、この画像データは、次いで、A/D変換される。A/D変換された画像データは演算処理端末9に入力され、前処理部2において前処理12を施される。

【0019】前処理においては、入力された画像データの色情度を削減し、画像の濃淡を2値化すると共にノイズを除去/平滑化して、ICカード8において処理すべきデータ量、照合に関する計算量を減少する。そして、一般に複数列のドットにより構成される画像の輪郭を細線化する画像データの整形することにより抽出された特徴点間の位置関係の演算処理を正確にしている。前処理部2においては、更に、指紋データ登録時の画像と指紋データ照合時の画像との間の位置補正を行う。

【0020】前処理12を施された画像データは、特徴データ抽出部3に入力され、特徴データ抽出13が実施される。特徴データ抽出部3により抽出された特徴データは暗号部6において暗号化され、暗号化された特徴データは演算処理端末9側からICカード8側に特徴データ送信14される。実施例の場合、暗号部6において暗号化された特徴データは復号部7により入力され、復号化される。一方において、特徴データ格納部10から格納されている暗号化特徴データを読み出し、これを復号部7に入力して復号化する。即ち、復号部7は、特徴データ抽出部3により抽出された特徴データを暗号部6よりより暗号化された特徴データを入力すると共に持筆者のICカード8の特徴データ格納部10に登録されている特徴データを入力して両暗号化特徴データを復号化する。照合部5は、復号化された両特徴データを入力して両特徴データを比較照合する。この場合、ICカード8内に格納されている登録データは、ICカード8に内蔵されるCPUが有するICカード8固有の照合プログラムからのみアクセスすることができる構成とし、一切ICカード8から外へ出力されることはない。照合の割合が或る閾値より大ければ照合成功、閾値より小ければ照合失敗とし、本人認証判断26して照合結果を演算処理端末9に返す。

【0021】以上の説明は、身体的特徴は指紋であるものとしてなされているが、これは指紋の他に、声紋、虹彩、筆跡の如きバイオメトリクスデータから選択した何れかであるものとして行うことができる。そして、身体的特徴として指紋、声紋、虹彩、筆跡の如きバイオメトリクスデータの複数個の組み合わせを使用することができ、これにより本人認証のセキュリティは更に向上する。

【0022】

【発明の効果】この発明によれば、ICカードを携帯することと、ICカードの携帯者がカード内の本来の所有者の身体的特徴のデータと照合することにより、極めてセキュリティの高い本人認証が行われる。そして、身体的特徴のデータを、指紋、声紋、虹彩、筆跡の如きバイオメトリクスデータから選択した複数個の組み合わせとすることにより、本人認証のセキュリティはより向上する。

【0023】また、演算処理端末において、特徴データ抽出部に前処理部を具備せしめ、入力される画像データのデジタル化、画像の色数の削減、ノイズの除去、画像の位置補正を行うことにより、身体的特徴のデータの処理量をICカードに組み込まれるCPUの演算処理能力内におさめることができる。更に、演算処理端末は特徴データ抽出部により抽出された特徴データを暗号化することにより、本人認証のセキュリティは更に向上する。

【0024】ここで、ICカードにおける特徴データの*

*登録読み出し処理、復号化処理、比較照合処理をICカードの内蔵するCPUの照合プログラムにより実施する構成とすることにより、ICカード内の所有者の特徴データがICカード外に出力されることはないので、特徴データを偽造することはできない。そして、身体的特徴のデータ、特に指紋は犯罪を連想させることもあり、本人の特徴データがICカードから外に出力されないことは心理的にも好適である。

【図面の簡単な説明】

【図1】実施例を説明する図。

【図2】指紋データを登録するときの処理を説明する図。

【図3】指紋データを照合するときの処理を説明する図。

【図4】従来例を説明する図。

【符号の説明】

- 1 指紋センサ
- 2 前処理部
- 3 特徴データ抽出部
- 4 格納処理部
- 5 照合部
- 6 暗号部
- 7 復号部
- 8 ICカード
- 9 演算処理端末
- 10 特徴データ格納部

【図1】

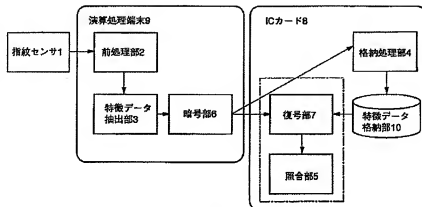


図 1

【図2】

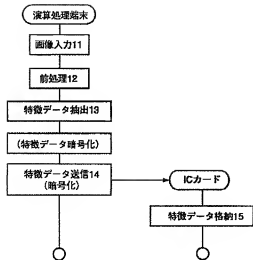


図 2

【図3】

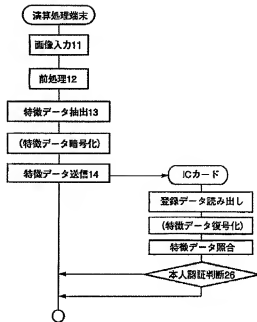


図 3

【図4】

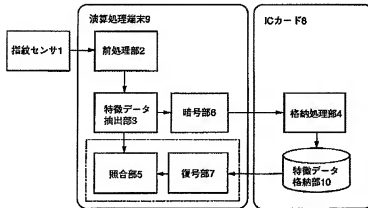


図 4

フロントページの続き

(72)発明者 細田 泰弘
東京都千代田区大手町二丁目3番1号 日
本電信電話株式会社内

Fターム(参考) 5B085 AE12 AE23 AE25 AE29
5J104 AA07 AA47 KA01 KA16 KA17
KA18 KA19 NA35 NA36 NA38
NA42 PA07 PA15

整理番号 502757
発送番号 002353
発送日 平成22年 1月 5日

拒絶査定

特許出願の番号	特願2003-372722
起案日	平成21年12月28日
特許庁審査官	鳥居 稔 4056 5500
発明の名称	情報保持装置
特許出願人	富士フイルム株式会社
代理人	龍華 明裕

この出願については、平成21年 3月27日付け拒絶理由通知書に記載した理由B.によって、拒絶をすべきものです。

なお、意見書及び手続補正書の内容を検討しましたが、拒絶理由を覆すに足りる根拠が見いだせません。

備考

出願人は、意見書において、請求項1に係る発明は、要求者が所有する要求者情報保持装置から取得した要求者特徴情報及び撮像部が生成した要求者特徴情報を用いて要求者の認証処理を行うのに対して、引用文献1及び2に記載された発明には、前記認証処理を行う構成は開示されておらず、引用文献から容易に発明できたとは考えられない旨主張している。

しかしながら、生体認証技術において、利用者の身体的特徴を撮像した画像データと、利用者のICカードから取得した身体的特徴データとを用いて利用者の認証を行うことは、引用文献4（特に、段落【0003】－【0006】等を参照）に記載されているように周知技術である。

そして、引用文献1に記載の発明において、上記周知技術を採用し、患者のICカードが、医師のICカードからのアクセス要求を検証して医師の認証を行う際に、ICカードから取得した医師の身体的特徴データと、医師を撮像して生成された身体的特徴データとを用いて認証する構成とすることは、当業者が容易に推考し得ることである。

また、引用文献1に記載の発明に上記周知技術を採用することによる効果も格別のことでない。

したがって、請求項1－4に係る発明は、引用文献1－3に記載された発明及び周知技術に基づいて、当業者が容易に発明することができたものであるから、特許法第29条第2項の規定により特許を受けることができない。

引用文献等一覧

1. 特開2001-257668号公報
2. 特開2001-195146号公報
3. 特開2002-133384号公報
4. 特開2001-202336号公報

この査定に不服があるときは、この査定の謄本の送達があった日から3月以内（在外者にあつては、4月以内）に、特許庁長官に対して、審判を請求することができます（特許法第121条第1項）。

（行政事件訴訟法第46条第2項に基づく告示）

この査定に対しては、この査定についての審判請求に対する審決に対してのみ取消訴訟を提起することができます（特許法第178条第6項）。

上記はファイルに記録されている事項と相違ないことを認証する。

認証日 平成22年 1月 4日 経済産業事務官 吉越 誠